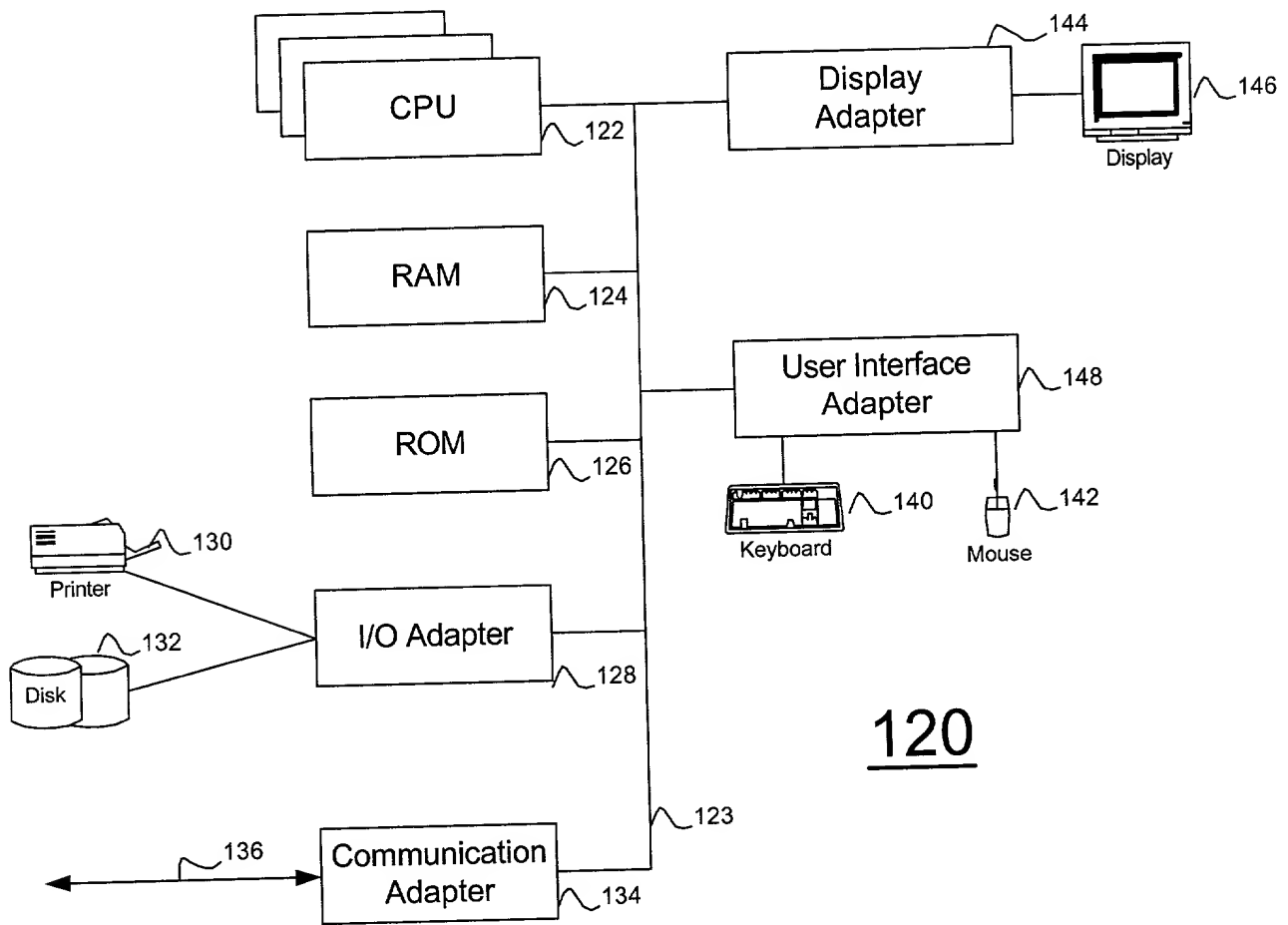
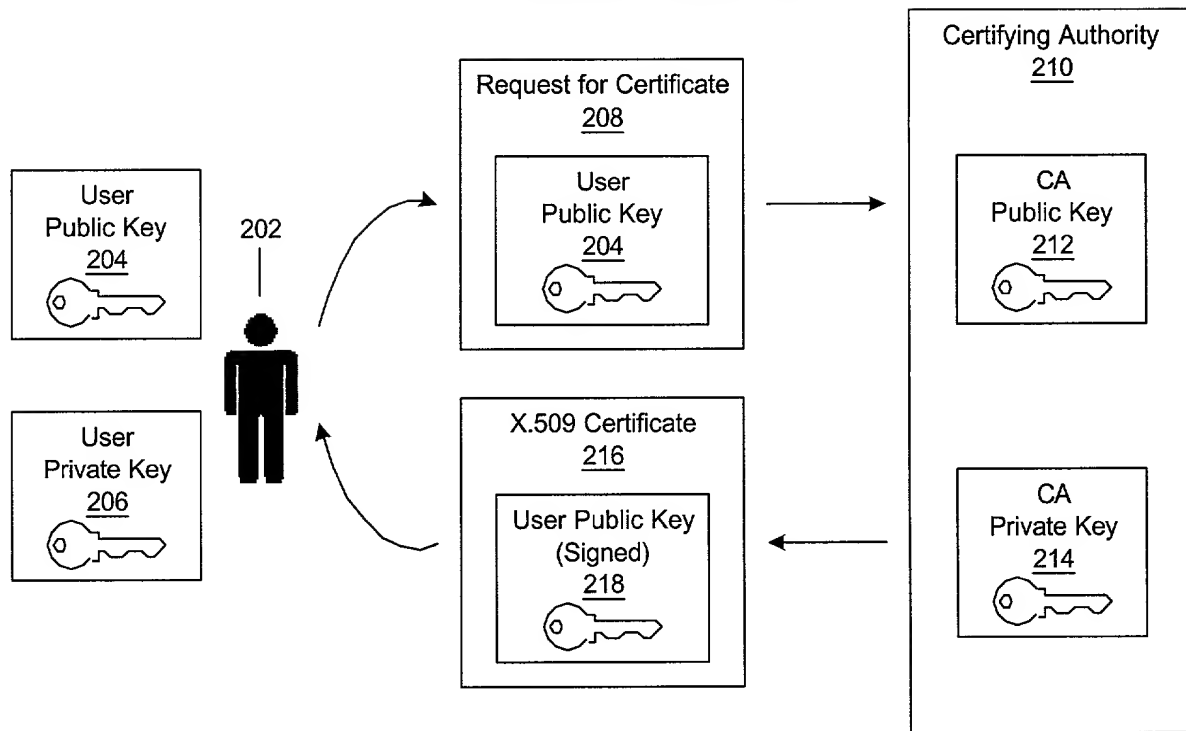


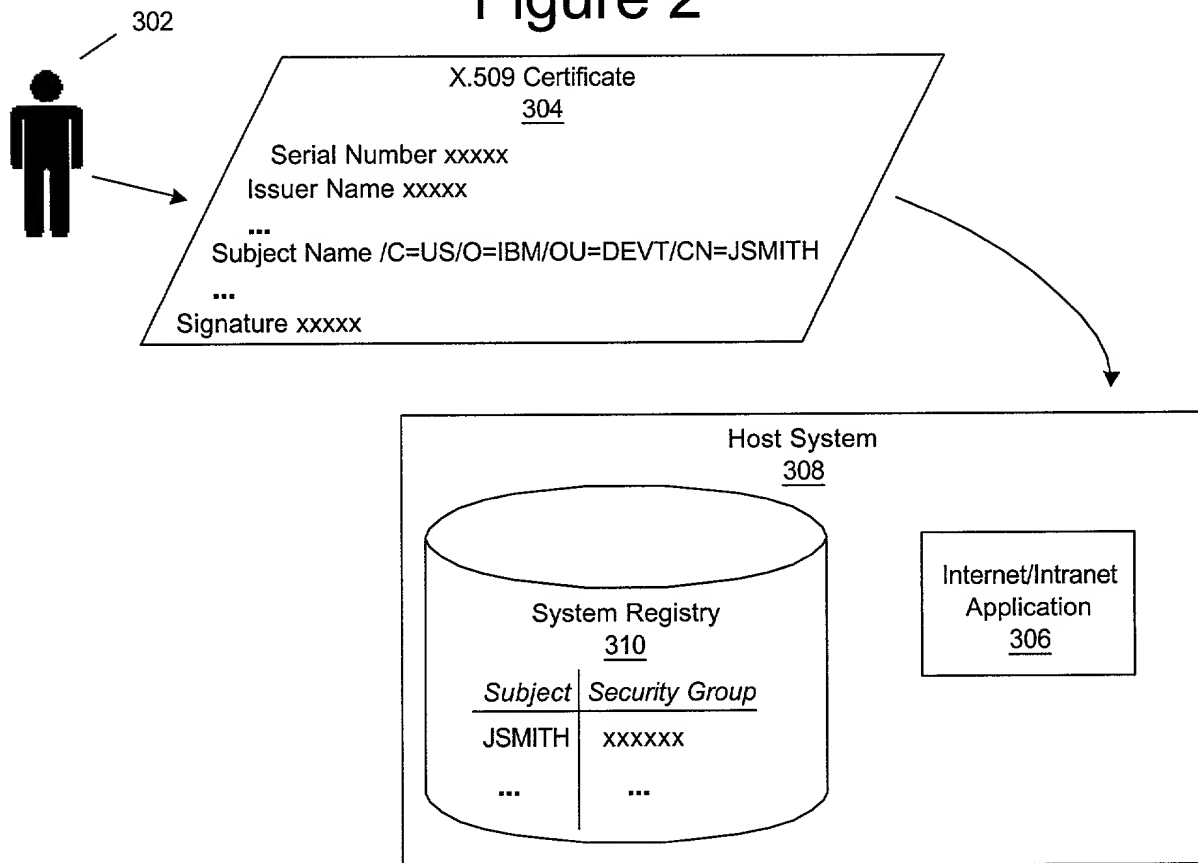
Prior Art
Figure 1A



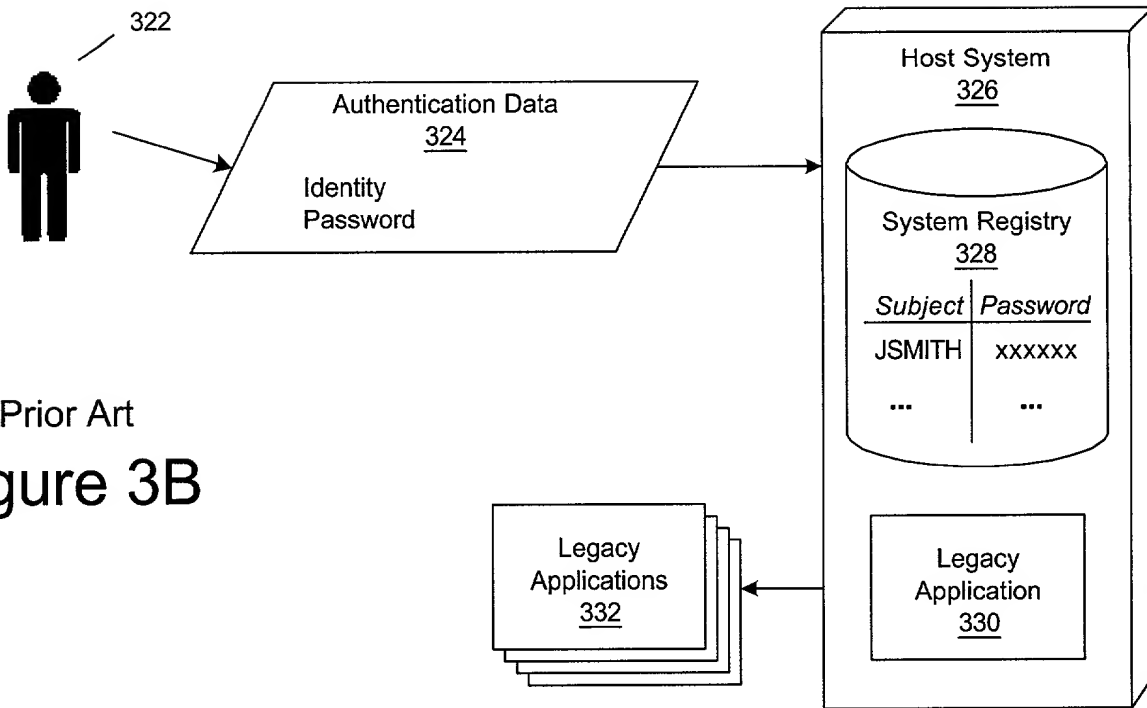
Prior Art
Figure 1B



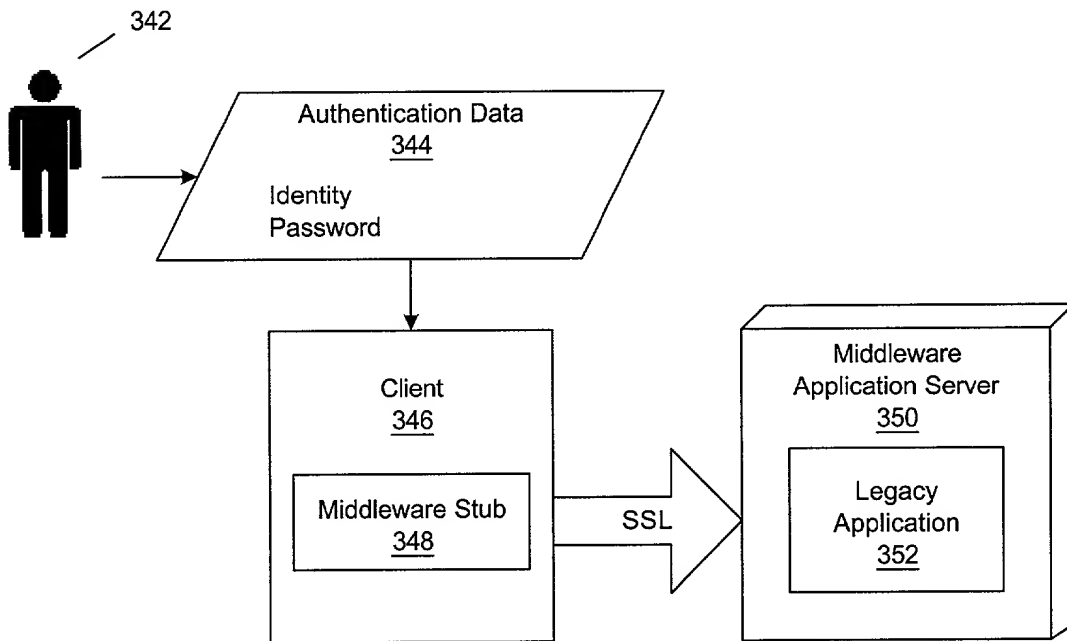
Prior Art
Figure 2



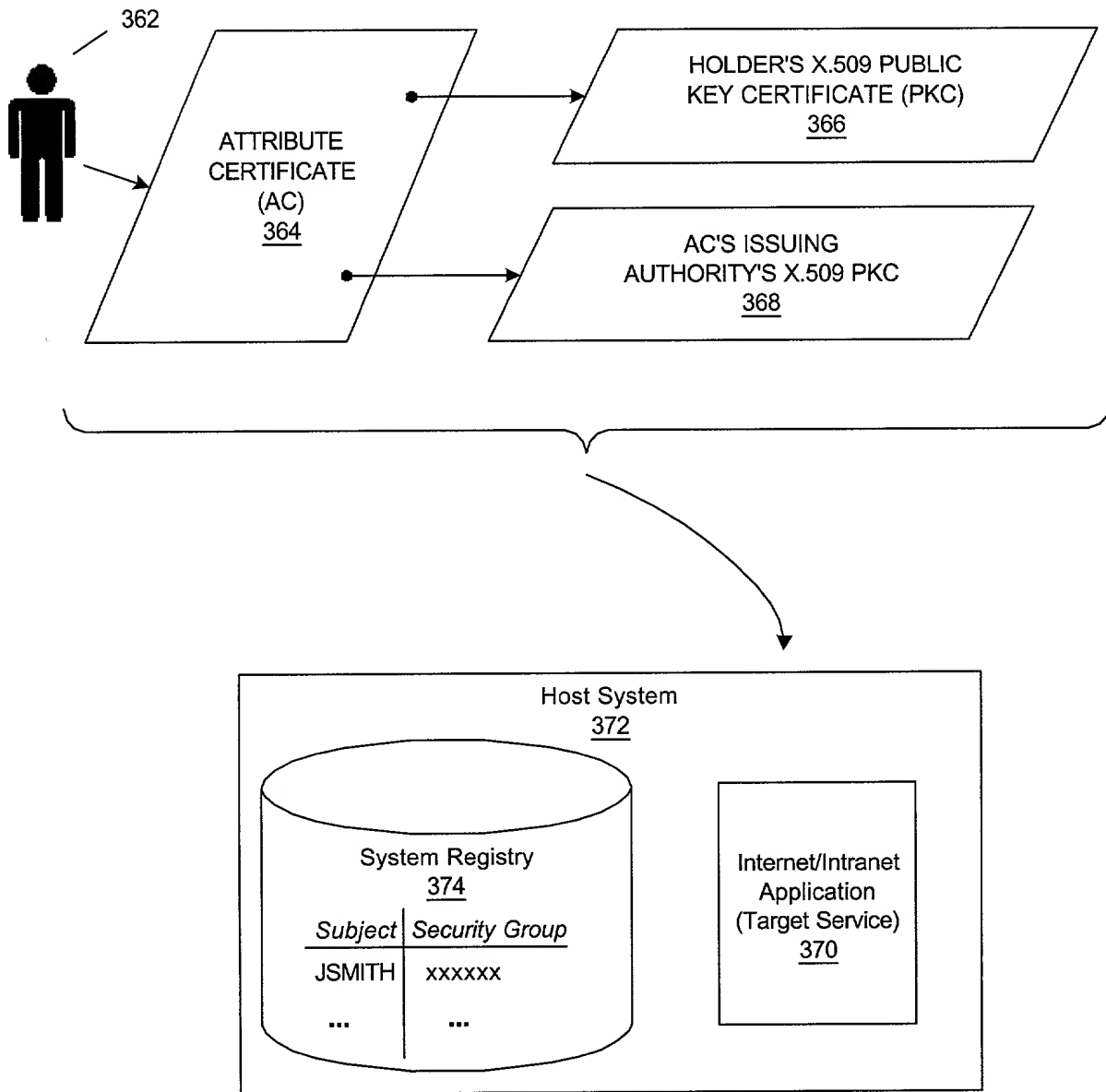
Prior Art
Figure 3A



Prior Art
Figure 3B



Prior Art
Figure 3C



Prior Art
Figure 3D

6/11
AUS920010064US1

Certificate ::= SEQUENCE {
 tbsCertificate TBSertificate,
 signatureAlgorithm AlgorithmIdentifier,
 signature BIT STRING }

TBSertificate ::= SEQUENCE {
 version [0] Version DEFAULT v1,
 serialNumber CertificateSerialNumber,
 signature AlgorithmIdentifier,
 issuer Name,
 validity Validity,
 subject Name,
 subjectPublicKeyInfo SubjectPublicKeyInfo,
 issuerUniqueID [1] IMPLICIT UniqueIdentifier OPTIONAL,
 subjectUniqueID [2] IMPLICIT UniqueIdentifier OPTIONAL,
 extensions [3] Extensions OPTIONAL }

Version ::= INTEGER { v1(0), v2(1), v3(2) }

CertificateSerialNumber ::= INTEGER

Validity ::= SEQUENCE {
 notBefore Time,
 notAfter Time }

Time ::= CHOICE {
 utcTime UTCTime,
 generalTime GeneralizedTime }

UniqueIdentifier ::= BIT STRING

SubjectPublicKeyInfo ::= SEQUENCE {
 algorithm AlgorithmIdentifier,
 subjectPublicKey BIT STRING }

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {
 extnID OBJECT IDENTIFIER,
 critical BOOLEAN DEFAULT FALSE,
 extnValue OCTET STRING }

Prior Art
Figure 4A

FIGURE 4A OF 6

7/11
AUS920010064US1

```
AttributeCertificate ::= SEQUENCE {
    acinfo          AttributeCertificateInfo,
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue   BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE {
    version          AttCertVersion DEFAULT v1,
    holder           Holder,
    issuer           AttCertIssuer,
    signature        AlgorithmIdentifier,
    serialNumber     CertificateSerialNumber,
    attrCertValidityPeriod AttCertValidityPeriod,
    attributes       SEQUENCE OF Attribute,
    issuerUniqueID   UniqueIdentifier OPTIONAL,
    extensions       Extensions OPTIONAL
}

AttCertVersion ::= INTEGER { v1(0), v2(1) }

Holder ::= SEQUENCE {
    baseCertificateID [0] IssuerSerial OPTIONAL,
    -- the issuer and serial number of
    -- the holder's Public Key Certificate
    entityName        [1] GeneralNames OPTIONAL,
    -- the name of the claimant or role
    objectDigestInfo  [2] ObjectDigestInfo OPTIONAL
    -- if present, version must be v2
}

ObjectDigestInfo ::= SEQUENCE {
    digestedObjectType ENUMERATED {
        publicKey          (0),
        publicKeyCert      (1),
        otherObjectTypes   (2) },
    -- otherObjectTypes MUST NOT
    -- be used in this profile
    otherObjectTypeID    OBJECT IDENTIFIER OPTIONAL,
    digestAlgorithm      AlgorithmIdentifier,
    objectDigest         BIT STRING
}
```

Prior Art
Figure 4B

8/11
AUS920010064US1

AttCertIssuer ::= CHOICE {
 v1Form GeneralNames, -- v1 or v2
 v2Form [0] V2Form -- v2 only
}

V2Form ::= SEQUENCE {
 issuerName GeneralNames OPTIONAL,
 baseCertificateID [0] IssuerSerial OPTIONAL,
 objectDigestInfo [1] ObjectDigestInfo OPTIONAL
 -- at least one of issuerName, baseCertificateID
 -- or objectDigestInfo MUST be present
}

IssuerSerial ::= SEQUENCE {
 issuer GeneralNames,
 serial CertificateSerialNumber,
 issuerUID UniqueIdentifier OPTIONAL
}

AttCertValidityPeriod ::= SEQUENCE {
 notBeforeTime GeneralizedTime,
 notAfterTime GeneralizedTime
}

Attribute ::= SEQUENCE {
 type AttributeType,
 values SET OF AttributeValue
 -- at least one value is required
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType

Prior Art
Figure 4C

name id-aca-authenticationInfo
OID { id-aca 1 }
Syntax SvceAuthInfo
values: Multiple allowed

SvceAuthInfo ::= SEQUENCE {
 service GeneralName,
 ident GeneralName,
 authInfo OCTET STRING OPTIONAL
}

Prior Art
Figure 4D

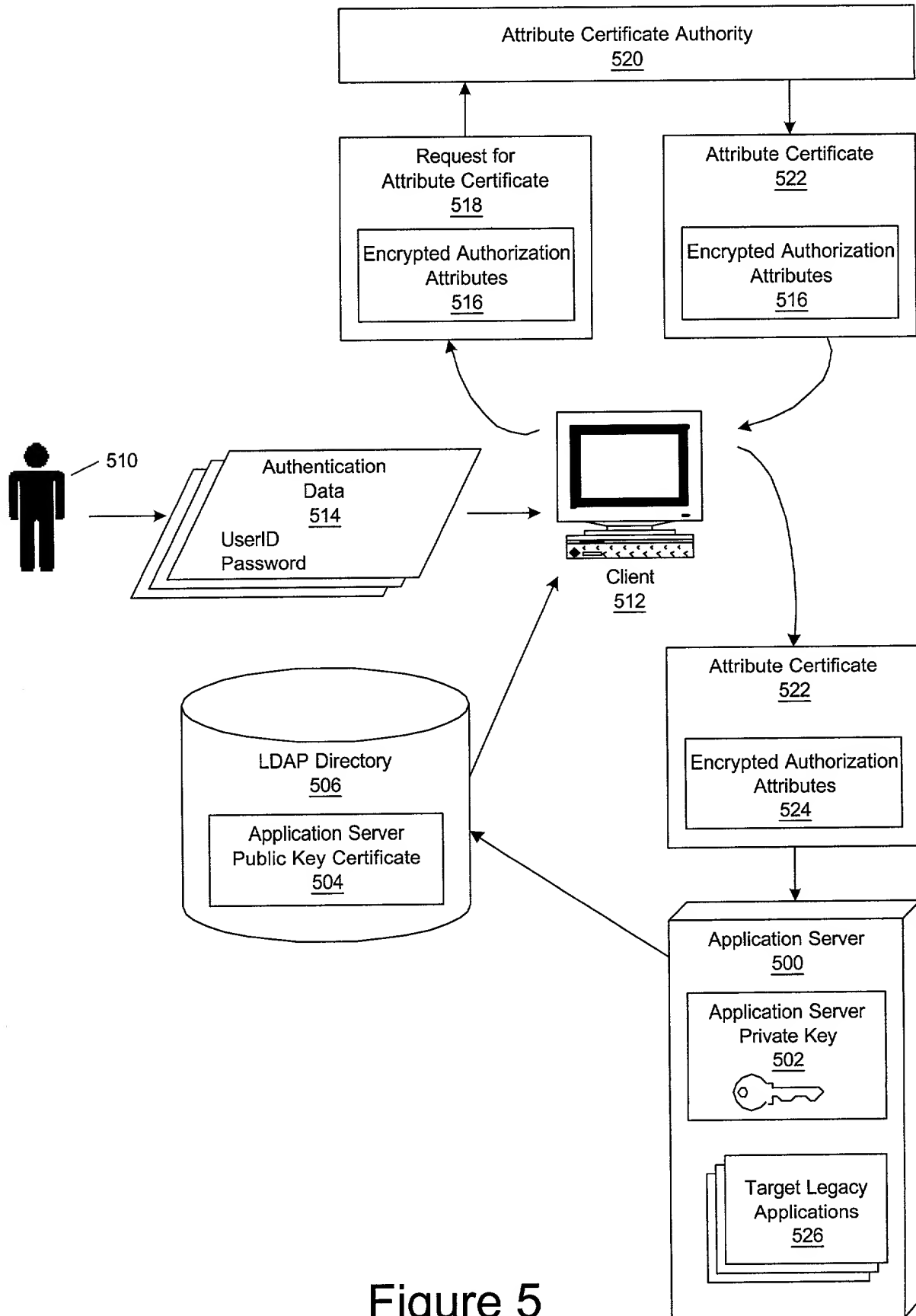


Figure 5

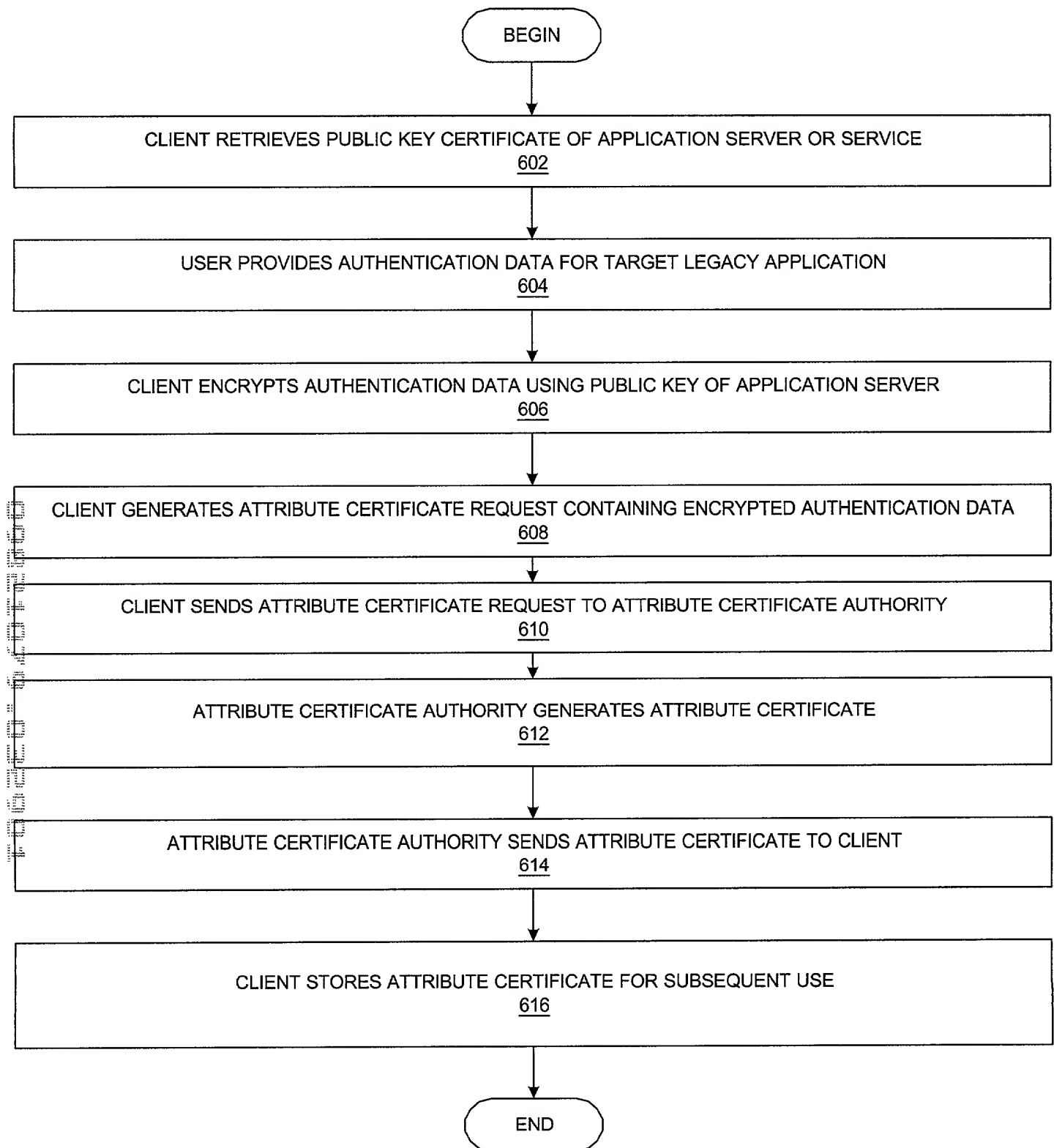


Figure 6

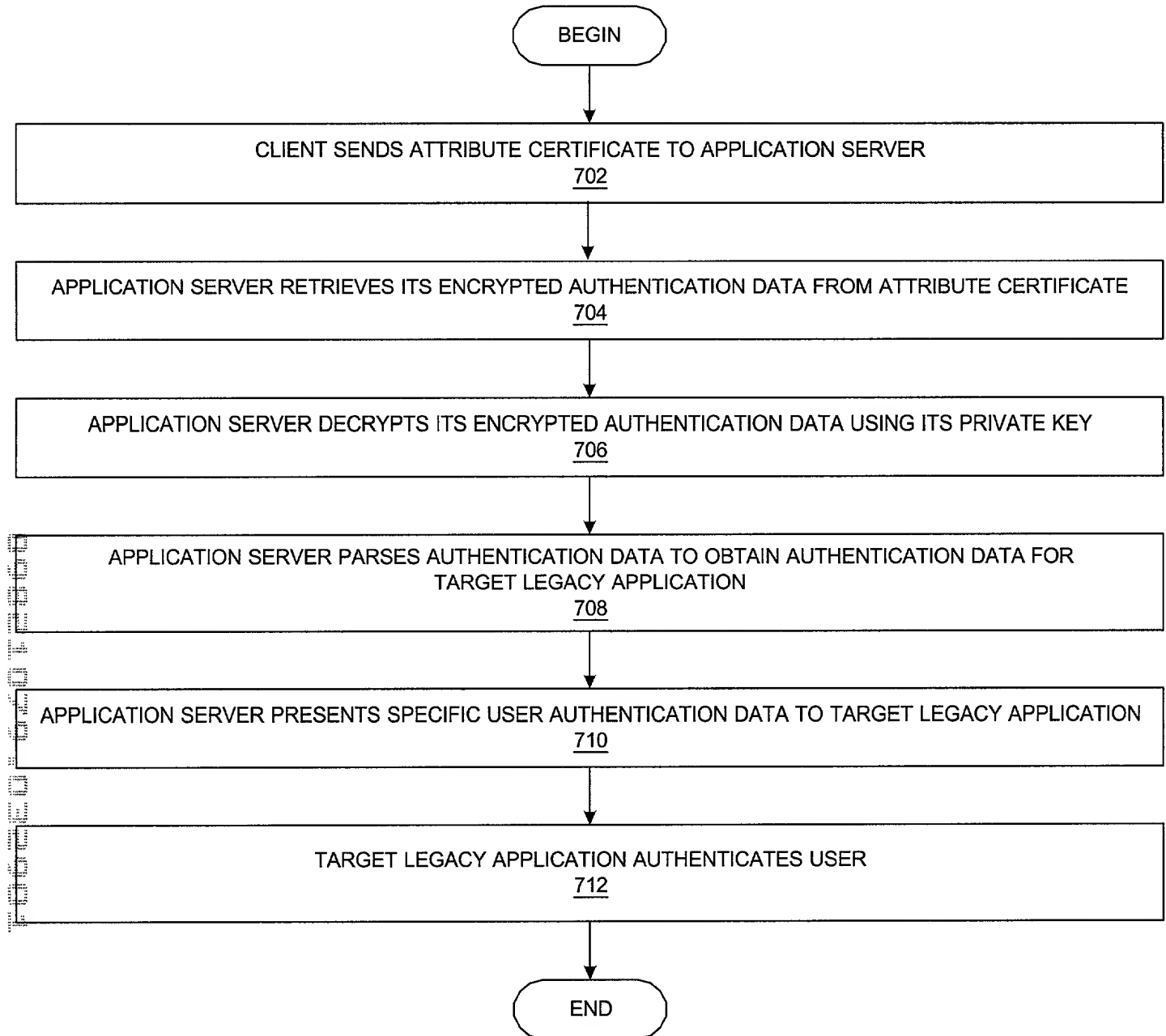


Figure 7